UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/659,864	09/12/2000	J. Leslie Vogel III	0044860.P2436	5866

7590 08/11/2004

Sheryl Sue Holloway
Blakely Sokoloff Taylor & Zafman LLP
12400 Wilshire Boulevard &th Floor
Los Angeles, CA 90025

EXAMINER	
TRAN, TONGOC	

ART UNIT	PAPER NUMBER
2134	3

DATE MAILED: 08/11/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/659,864	Applicant(s) VOGEL, J. LESLIE	
	Examiner Tongoc Tran	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 September 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-45* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 2.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to applicant's application serial no. 09/659864 filed on 9/12/2000.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 12/6/2001 has been considered by the examiner.

Claim Objections

3. Claim 37 is objected to because of the following informalities:

On lines 3-4, the phrase, "...and the station is sending the authentication information to *the station* upon receiving a security preference specifying shared key". The underlined term "the station" appears to be a typographical error. For the purpose of prosecuting the case, examiner assumes that it is intended to be "the access point".

Appropriate correction is required.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which

said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-3, 9-17, 19-22, 24-27, 29-32, 34-38, and 40-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis (U.S. Patent No. 6,526,506) in view of Quick Jr. (U.S. Patent No. 6,178,506, hereinafter Quick).

In respect to claim 1, Lewis discloses a method of establishing a secure wireless communications channel between an access point and a station, the channel being encrypted with a channel key, the method comprising:

sending, by the station to the access point, a request for a security preference for the access point (see Lewis, col. 6, lines 43-58);

sending, by the access point to the station, the security preference in response to the request when the access point can support the channel (see Lewis, col. 6, lines 43-58);

sending, by the station to the access point, the authentication information (see Lewis, col. 4, lines 27-42);

validating, by the access point, the station using the authentication information; encrypting, by the access point, the channel key using a second key when the station is validated (see Lewis, col. 4, lines 27-42 and col. 5, lines 29-41);

sending, by the access point to the station, the encrypted channel key (see Lewis, col. 5, lines 29-41);

decrypting, by the station, channel key in response to receiving the encrypted channel key; and sending, by the station to the access point, data

encrypted with the channel key to establish the channel (see Lewis, col. 5, line 10-col. 6, line 17).

Lewis discloses the mobile terminal sending authentication information (registering) with the access point (see Lewis, col. 4, lines 28-35) but does not explicitly discloses encrypting the authentication information. However, Quick discloses encrypting authentication information from mobile terminal to access point (see Quick, col. 3, lines 1-10). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teaching of Quick's encrypting the authentication information with the teaching of Lewis' registering the mobile terminal with the access point in order to protect the use identification and password from compromise during the registration process (Quick, col. 2, lines 46-9).

In respect to claim 2, Lewis and Quick disclose the method of claim 1, wherein the first and second keys are a self-distributed key (see Quick, col. 4, line 45-col. 5, line 8).

In respect to claim 3, Lewis discloses the method of claim 1, Lewis wherein the first and second keys are a self distributed key and further comprising:

generating, by the access point, the self-distributed key using a security algorithm when the security preference is shared key; generating, by the station and sending to the access point, a first value using the security algorithm in response to receiving the security preference of shared key; generating, by the access point, and sending to the station, a second value using the security

algorithm and the first value in response to receiving the first value; and calculating, by the station, the self-distributed key using the security algorithm and the second value in response to receiving the second value (see Quick, col. 4, line 45-col. 5, line 8).

In respect to claim 9, Lewis and Quick disclose the method of claim 2 further comprising:

encrypting, by the station, a name and password with the first key to generate the authentication information; and decrypting, by the access point, the name and password to validate the station (see Quick, col. 4, line 45-col. 5, line 8).

In respect to claim 10, Lewis and Quick disclose the method of claim 2 further comprising:

sending, by the access point to the station, a challenge; encrypting, by the station, the challenge with the first key to generate the authentication information; encrypting, by the access point, the challenge with the first key; and comparing, by the access point, the authentication information with the challenge encrypted by the access point with the first key to validate the station (see Quick, col. 4, line 45-col. 5, line 8)

In respect to claim 11, Lewis and Quick disclose the method of claim 1, wherein the first key is a public key of a public-private key pair for the access point, and the second key is a public key of a public-private key pair for the station (see Quick, col. 4, line 45 –col. 5, line 8).

In respect to claim 12, Lewis and Quick disclose the method of claim 11 further comprising:

sending, by the access point to the station, the first key; and.

sending, by the station to the access point, the second key (see Quick col. 4, line 45-col. 5, line 8)

In respect to claim 13, Lewis and Quick disclose the method of claim 12, wherein the second key is sent to the access point when the request for the security preference is sent by the station (see Quick, col. 4, line 45-col. 5, line 8).

In respect to claim 14, Lewis and Quick disclose the method of claim 12, wherein the first key is sent to the station when the security preference is sent by the access point (see Quick, col. 4, line 45-col. 5, line 8).

In respect to claim 15, Lewis discloses the method of claim 1, wherein establishing the channel creates a standard wired equivalent privacy (WEP) network, and the station and the access point exchange messages conforming to a format required by the standard that defines a WEP network to establish the WEP network (see Lewis, col. 2, lines 18-43).

In respect to claim 16, 21, 26, 31 and 36-37, 40 and 42-45, the claim limitations are substantially similar to claim 1. Therefore, claims 16, 21, 26, 31, 36-37 and 40 are rejected based on the similar rationale.

In respect to claim 17, the claim limitation is substantially similar to claim 3. Therefore, claim 17 is rejected based on the similar rationale.

In respect to claim 19, the method of claim 16 further comprising:

using a first key to generate the authentication information; and

using a second key to decrypt the encrypted channel key (see Lewis, col. 5, line 10-col. 6, line 17).

In respect to claims 20, 25, 30, 35, and 41, the claim limitations are substantially similar to claim 11. Therefore, claims 20, 25, 30 and 35 are rejected based on the similar rationale.

In respect to claims 24, 29 and 34, the claim limitations are substantially similar to claim 19. Therefore, claims 24, 29 and 34 are rejected based on the similar rationale.

In respect to claim 22, the claim limitation is substantially similar to claim 3. Therefore, claim 22 is rejected based on the similar rationale.

In respect to claim 27, the claim limitation is substantially similar to claim 17. Therefore claim 27 is rejected based on the similar rationale.

In respect to claim 32, the claim limitation is substantially similar to claim 22. Therefore, claim 32 is rejected based on the similar rationale.

In respect to claim 38, Lewis and Quick disclose the secure wireless network of claim 37, wherein access point if further operable for encrypting the shared channel key using a self-distributed key for sending to the station and the station is further operable for decrypting the shared channel key upon receipt (see Quick, col. 4, line 45-col. 5, line 8).

5. Claims 4-8, 18, 23, 28, 33 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis (U.S. Patent No. 6,526,506) in view of Quick Jr. (U.S. Patent No. 6,178,506, hereinafter Quick) and further in view of Schneier

("Applied Cryptography, Second Edition, Protocols, Algorithms, and Source Code in C", John Wiley & Sons, Inc., 1996, hereinafter Schneier).

In respect to claim 4, Lewis and Quick disclose the method of claim 3. Lewis and Quick do not disclose but Schneier discloses wherein the security algorithm is g mod p and further comprising:

obtaining, by the access point, integers x, g and p to generate the self-distributed

key $k = g^x \bmod p$;

obtaining, by the station, the integers g and p, and an integer y to generate the first value $Y = g^x \bmod p$;

generating, by the access point, the second value $X = Y^x \bmod p$; and

setting, by the, z equal to $y^{-1}$to calculate the self-distributed key

$k = X^z \bmod p$ (see Schneier, page 515, Hughes).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Schneier with the teaching of Lewis's wireless communication between mobile and access point and Quick's Diffie-Hellman's protocol with Schneier's teaching of Hughes' protocol so that key can be computed before any interaction between the mobile station and the access point (see Schneier, page 515, Hughes and Key Exchange Without Exchanging Keys).

In respect to claim 5, Lewis, Quick and Schneier disclose the method of claim 4 wherein obtaining, by the station, the integers g and p comprises:

sending, by the access point (Bob) to the station (Alice), the integers for g and p (see Schneier, page 515, g and n).

In respect to claim 6, Lewis, Quick and Schneier disclose the method of claim 5, wherein the integers for g and p (g and n) are sent to the station (Alice) when the security preferences are sent by the access point (Bob) (see Schneier, page 515, Hughes).

In respect to claim 7, Lewis, Quick and Schneier disclose the method of claim 5, wherein g and p are sent to the station when a user name and password for the station are registered with the access point (see Quick, col. 4, line 60 to col. 5, line 8).

In respect to claim 8, Lewis, Quick and Schneier discloses the method of claim 4 further comprising:

publishing, by the access point, the integers g and p for a set of stations (see Schneier, page 515).

In respect to claims 18, 23, 28 and 33, the claim limitations are substantially similar to claim 4. Therefore, claims 18, 23, 28 and 33 are rejected based on the similar rationale.

In respect to claim 39, Lewis and Quick disclose the secure wireless network of claim 38. Lewis and Quick do not disclose but Schneier discloses wherein the station and the access point are further operable for calculating the self-distributed key by exchanging messages in accordance with the Hughes transmission protocol (see Schneier, page 515, Hughes). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was

made to modify the teaching of Schneier with the teaching of Lewis's wireless communication between mobile and access point and Quick's Diffie-Hellman's protocol with Schneier's teaching of Hughes' protocol so that key can be computed before any interaction between the mobile station and the access point (see Schneier, page 515, Hughes and Key Exchange Without Exchanging Keys).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

-Jablon discloses systems, methods and software for remote password authentication using multiple servers.

-Wang discloses authorization fireware for conducting transactions with an electronic transaction system and methods therefore.

-Wang discloses electronic transaction systems and methods therefor.

-Matias et al. Disclose simplified secure shared key establishment and data delivery protocols for electronic commerce.

-Brockmann discloses data communication network.

-Frerking discloses method for managing the registration of a wireless unit.

-Lewis discloses multi-level encryption system for wireless network.

-Morgan et al. Disclose security method and system for persistent storage and communications on computer network systems employing the same.

-Ala-Laurila et al. Disclose transfer of security association during a mobile terminal handover.

-Binding et al. Disclose piggy-backed key exchange protocol for providing secure, low-overhead browser connections to a server with which a client shares a message encoding scheme.

-Chuah discloses method for access control in a multiple access system for communications networks.

-Kuikka et al. disclose a method and associated apparatus for generating security keys in a communication system.

-Stenman et al. Disclose a key management methods for wireless LANS.

-Frerking discloses a wireless communication registration management system.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tongoc Tran whose telephone number is (703) 305-7690. The examiner can normally be reached on 8:30-5:00 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Examiner: Tongoc Tran
Art Unit: 2134

TT

August 2, 2004

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100